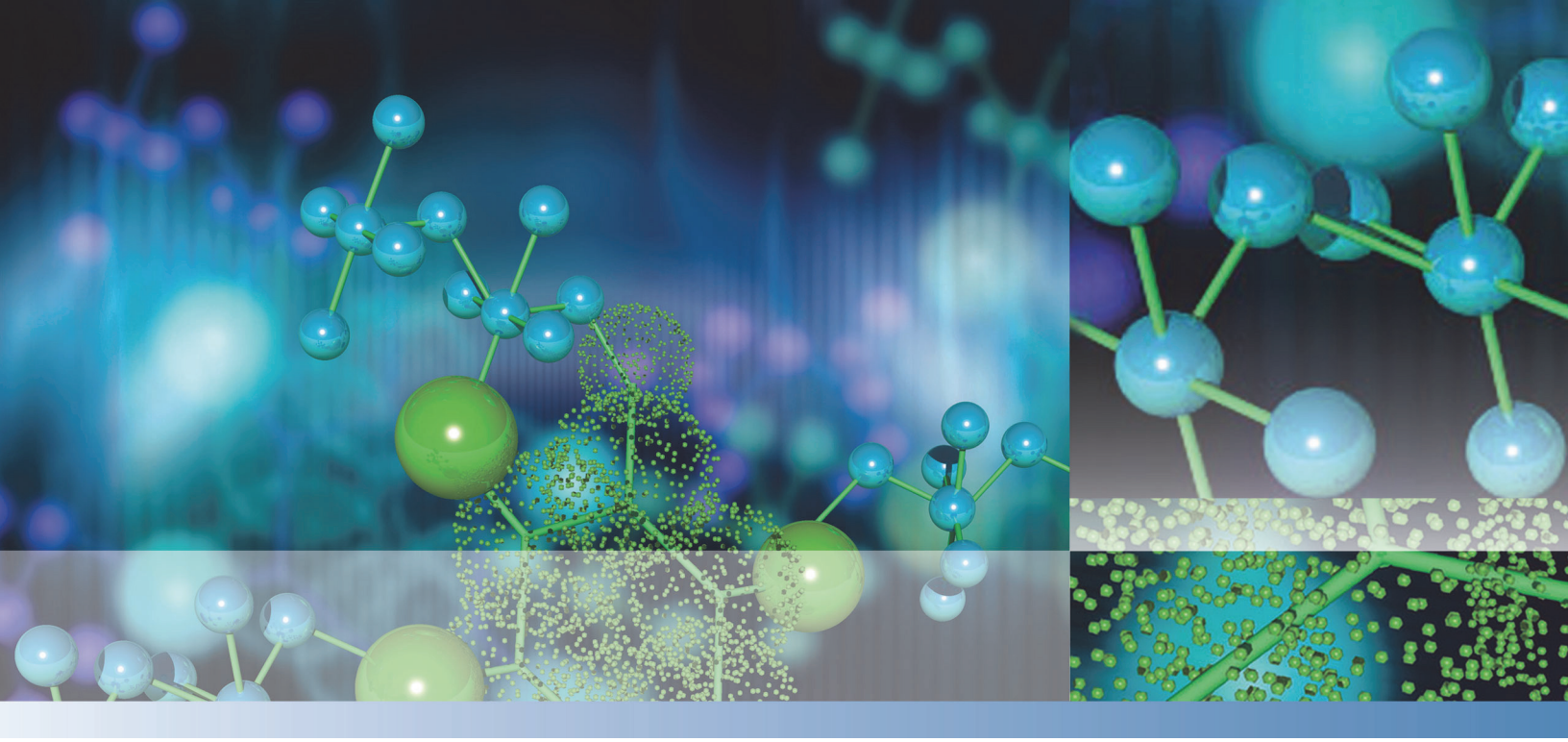


Thermo

TraceFinder

Administrator Console User Guide

Software Version 3.3

XCALI-97733 Revision A May 2015

DOCUMENTATION SURVEY

Thermo SCIENTIFIC

© 2015 Thermo Fisher Scientific Inc. All rights reserved.

TraceFinder is a trademark, and Thermo Scientific and Xcalibur are registered trademarks of Thermo Fisher Scientific Inc. in the United States.

NIST is a registered trademark of the National Institute of Standards and Technology in the United States.

The following are registered trademarks in the United States and other countries: Windows, Active Directory, Excel, and Microsoft are registered trademarks of Microsoft Corporation.

All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries.

Thermo Fisher Scientific Inc. provides this document to its customers with a product purchase to use in the product operation. This document is copyright protected and any reproduction of the whole or any part of this document is strictly prohibited, except with the written authorization of Thermo Fisher Scientific Inc.

The contents of this document are subject to change without notice. All technical information in this document is for reference purposes only. System configurations and specifications in this document supersede all previous information received by the purchaser.

This document is not part of any sales contract between Thermo Fisher Scientific Inc. and a purchaser. This document shall in no way govern or modify any Terms and Conditions of Sale, which Terms and Conditions of Sale shall govern all conflicting information between the two documents.

Release history: Revision A, May 2015

Software version: Microsoft Windows 7 Professional SP1; (Thermo) Foundation 3.1; Xcalibur 3.1; LC Devices 3.0; GC Devices 3.2

For Research Use Only. Not for use in diagnostic procedures.

Contents

Preface . . . . . **v**
Contacting Us vii
Accessing the Administrator Console viii

Chapter 1 Using the Security View **1**
Authentication Provider 1
Global Policy 3
Users 6
Roles 8
Role Mapping 18

Chapter 2 Using the Repository View **21**
Administration 21
Domain Mapping 24

Chapter 3 Using the Audit View **25**
Audit Logs 25
Event Maps 26

Chapter 4 Using the Plugins View **33**

Appendix A Importing and Exporting Administrator Settings **37**

Index **39**

P

Preface

This guide discusses the features of the Thermo TraceFinder™ Administrator Console. This console is available to any user with Administrator permission.

If you are a member of the local administrator's group and are launching the TraceFinder application for the first time, you will have Administrator permissions. See "Role Permission Defaults" on page 16.

Contents

- Related Documentation
- Special Notices
- Contacting Us
- Accessing the Administrator Console

Related Documentation

The TraceFinder application includes Help and these manuals as PDF files:

- *TraceFinder User Guide*
- *TraceFinder Administrator Console User Guide*
- *TraceFinder Acquisition Quick Reference Guide*
- *TraceFinder Analysis Quick Reference Guide*
- *TraceFinder Shortcut Menus Quick Reference Guide*

❖ **To view TraceFinder documents using the Start menu**

From the Microsoft™ Windows™ taskbar choose **Start > All Programs > Thermo TraceFinder > Manuals**.

❖ **To open TraceFinder Administrator Console Help**

Click the **Help** icon, .

Special Notices

This guide includes the following types of special notices:

IMPORTANT Highlights information necessary to prevent damage to software, loss of data, or invalid test results; or might contain information that is critical for optimal performance of the system.

Note Highlights information of general interest.

Tip Highlights helpful information that can make a task easier.

Contacting Us

There are several ways to contact Thermo Fisher Scientific for the information you need. You can use your smartphone to scan a QR code, which opens your email application or browser.

Contact us	Customer Service and Sales	Technical Support
	(U.S.) 1 (800) 532-4752	(U.S.) 1 (800) 532-4752
	(U.S.) 1 (561) 688-8731	(U.S.) 1 (561) 688-8736
	us.customer-support.analyze@thermofisher.com	us.techsupport.analyze@thermofisher.com

❖ **To find global contact information or customize your request**

1. Go to Thermoscientific.com.
2. Click **Contact Us**, select the **Using/Servicing a Product** option, and then type the product name.
3. Use the phone number, email address, or online form.

❖ **To find product support, knowledge bases, and resources**

Go to www.thermoscientific.com/support.

❖ **To find product information**

Go to www.thermoscientific.com/lc-ms.

Note To provide feedback for this document:

- Send an email message to Technical Publications (techpubs-lcms@thermofisher.com).
- Complete a survey at www.surveymonkey.com/s/PQM6P62.

Accessing the Administrator Console

The Administrator Console is available from the Tools menu in any TraceFinder application window or from the Windows™ Start menu when you install the TraceFinder application.

Follow these procedures:

- To log in to the Administrator Console when user security is not enabled
- To log in to the Administrator Console when user security is enabled

❖ To log in to the Administrator Console when user security is not enabled

1. Do one of the following:

   - Choose **Start > All Programs > Thermo TraceFinder > TraceFinder Administration Console**.

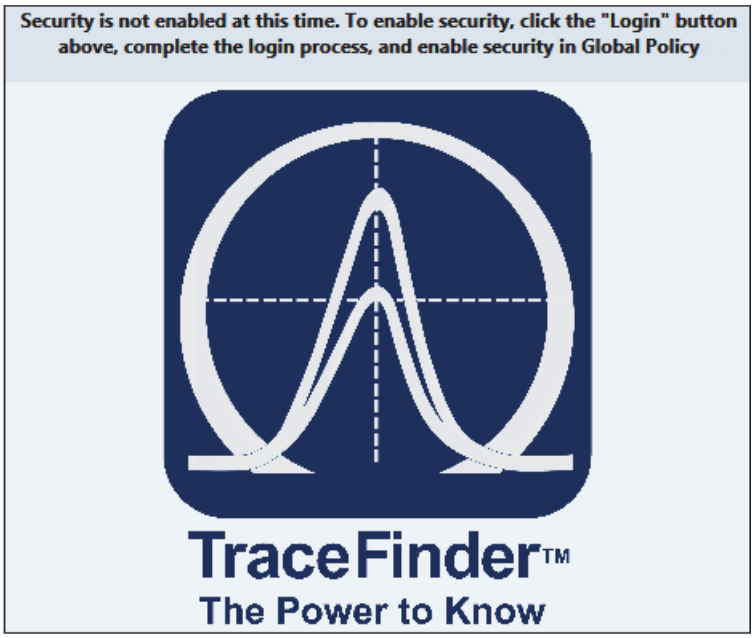
   –or–

   - Choose **Tools > Administrator Console** from the TraceFinder main menu.

   –or–

   - Double-click the **TraceFinder Administration Console** icon on your desktop, .

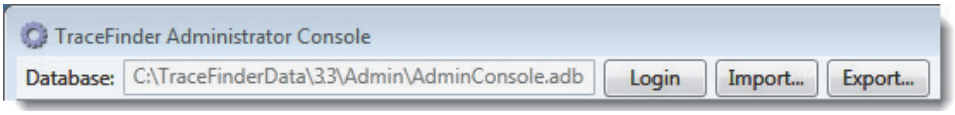
   The TraceFinder Administrator Console window opens, notifying you that user security is not enabled.


Security is not enabled at this time. To enable security, click the "Login" button above, complete the login process, and enable security in Global Policy
TraceFinder™
The Power to Know

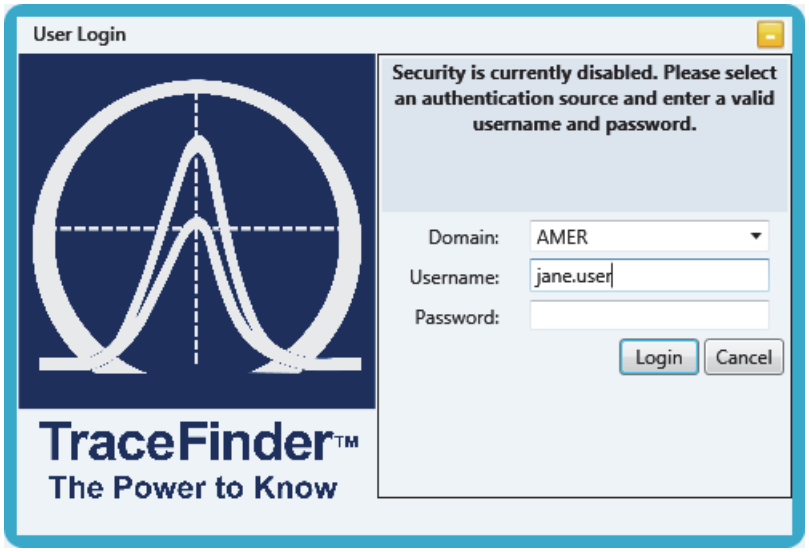
   You can proceed without enabling user security, and still have access to all Administrator Console features except the Security features.

2. To access the Security features, do the following:

   a. Click **Login**.



   The User Login dialog box opens.



   Note You must enter a valid user name and password before you can access the Security features.

   b. Select your domain, either your Windows Active Directory™ domain or your local windows computer name.

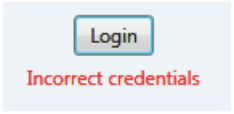
   c. Type your user name.

   d. Type your password.

   e. Click **Login**.

      The application authenticates your login and password and opens the TraceFinder Administrator Console.

      If the authentication fails, the application displays Incorrect Credentials.



      The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

3. To turn on user security, requiring all users to log in each time they launch the TraceFinder application, see "To enable security" on page 3.

❖ To log in to the Administrator Console when user security is enabled

1. Do one of the following:

   - Choose **Start > All Programs > Thermo TraceFinder > TraceFinder Administration Console**.

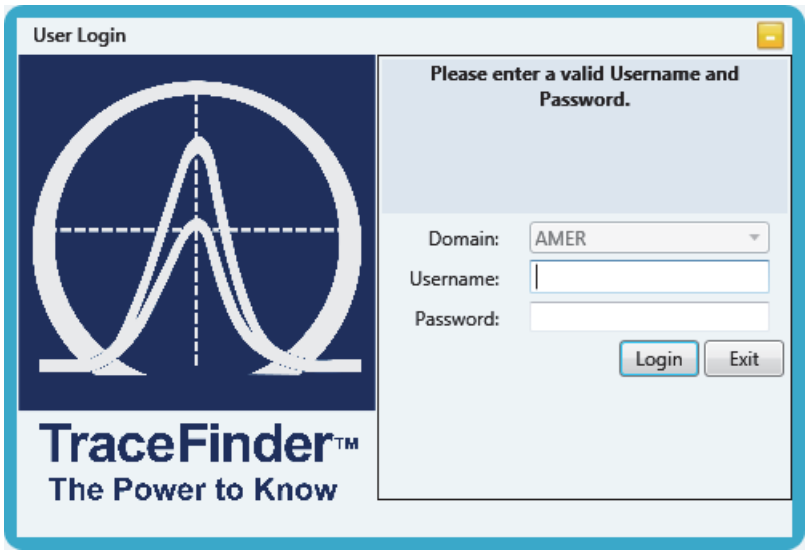
   –or–

   - Choose **Tools > Administrator Console** from the TraceFinder main menu.

   –or–

   - Double-click the **TraceFinder Administration Console** icon on your desktop, .

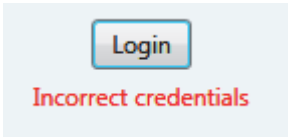
   The TraceFinder Administrator Console window opens to the User Login page.



2. Select your domain, either your Windows Active Directory domain or your local windows computer name.
3. Type your user name.
4. Type your password.
5. Click **Login**.

   The application authenticates your login and password and opens the TraceFinder Administrator Console.

   If the authentication fails, the application displays Incorrect Credentials.



   The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

Administrator Console

You can access the following functions of the Administrator Console from the left navigation pane and the top menu bar.

Function	Description
Security	Use the Security view to specify how the application manages authentication, to create and manage users, to map groups to roles and roles to users, or to select specific permissions for all user roles. See "Using the Security View" on page 1.
Repository	Use the Repository view to specify repositories for batches, methods, or templates that you create. See "Using the Repository View" on page 21.
Plugins	Use the Plugins view to configure available plugins for the TraceFinder application. See "Using the Plugins View" on page 33.
Import/Export	Use the Export button to save your current security settings to a file. Use the Import button to import saved security settings to your current Administrator Console. See "Importing and Exporting Administrator Settings" on page 37.

1

Using the Security View

When security is enabled, a user with Security permission can choose authentication providers, specify how the application manages authentication, create and manage users, map groups to roles and roles to users, and select specific permissions for all user roles.

Contents

- Authentication Provider
- Global Policy
- Users
- Roles
- Role Mapping

Authentication Provider

Use the features on the Security – Authentication Provider page to select a method for authenticating user security.

❖ **To specify how user authentication is implemented**

1. Click **Authentication Provider** in the navigation pane.

   The Security – Authentication Provider page opens.

Security - Authentication Provider
Authentication Provider
Local Windows
Active Directory Domain AMER
Select...
Active Directory authentication queries the local Active Directory to perform security authentication operations. Groups or users which are mapped to TraceFinder roles must exist as Active Directory user or group objects.

   The application displays the current authentication provider.

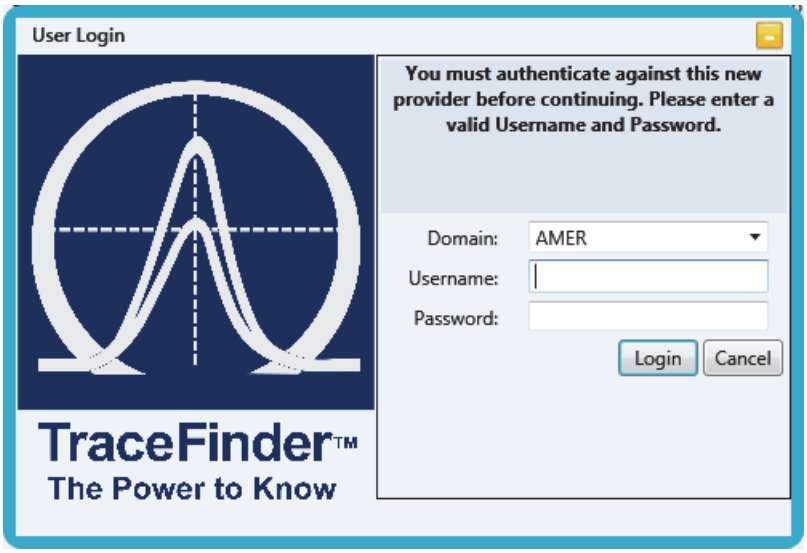
   - **Local Windows**: Uses the local Windows user login and password to allow access to the TraceFinder application. To be allowed access, users must have a Windows user account on the local machine.

- **Active Directory Domain**: Uses the selected Active Directory domain to allow access to the TraceFinder application. To be allowed access, users must be members of the selected domain.

To activate these options for user authentication, you must enable security on the Security – Global Policy page. See Global Policy.

2. To choose a different authentication provider, click **Select**.

   The User Login dialog box opens.



3. Select a domain.
4. Type your user name and password for the selected domain.
5. Click **Login**.

   The application authenticates the specified domain, user name, and password. If the authentication fails, enter your user name and password again or click **Cancel** to remained logged in to the current domain.

Global Policy

Use the features on the Security – Global Policy page for controlling user security, automatic logoff, and access to the TraceFinder application.

Follow these procedures:

- To open the Global Policy page
- To enable security
- To enable automatic screen locking
- To restrict access only to users created in TraceFinder
- To allow access without logging in

❖ To open the Global Policy page

Click **Global Policy** in the navigation pane.

The Security – Global Policy page opens. For detailed descriptions of all the global policy parameters, see "Security – Global Policy Page" on page 5.

❖ To enable security

1. Select the **Enable Security** check box.

   The application enables the features in the Security view.

2. Click **Apply**.

   When you enable user security, users must log in with their user name and password. The application uses the authentication method you specify to authenticate the user name and password.

❖ To enable automatic screen locking

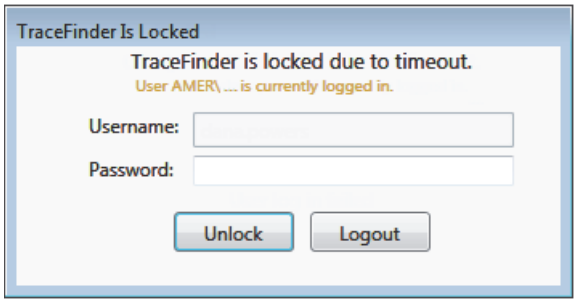
1. Select the **Lock Client...** check box.

   Note This feature is available only when you select the **Enable Security** check box.

2. In the Minutes box, type the number of minutes of inactivity before the application locks the screen and prompts the user to reenter the password.

   You can enter a number between 1 and 999 minutes. (999 minutes is approximately 16 hours.)

After the specified number of minutes elapses with no activity from a user, the TraceFinder application displays a lock screen with this login box.



While the password-protected lock screen is active, the TraceFinder application continues to perform all queued analysis, acquisition, processing, or reporting functions.

3. When you have completed all your changes to the Security – Global Policy page, click **Apply**.

❖ To restrict access only to users created in TraceFinder

1. Select the **Authenticate Explicit Users Only** check box.

   Note This feature is available only when you select the **Enable Security** check box.

2. Click **Apply**.

   The TraceFinder application allows access only to users listed in the Users list on the Users page. See "Users" on page 6. Users cannot access the application simply by being included in a local Windows security group or Active Directory.

❖ To allow access without logging in

1. Select the **Silent Authentication** check box.

   Note This feature is available only when you select the **Enable Security** check box.

2. Click **Apply**.

   Even when user security is enabled, a user who is currently logged in to a local machine can access the TraceFinder application without logging in again. The TraceFinder application authenticates the user without requiring a user name and password.

Security – Global Policy Page

From the Security – Global Policy page, you can set parameters for user security, automatic logoff, and access to the TraceFinder application.

Figure 1. Security – Global Policy page

Security - Global Policy
Enable Security
Lock client that has no interaction for 5 minutes.
After lockout, the current user can log back in or log out.
Authenticate explicit users only.
Authenticate only those users who are explicitly listed under Users tab.
Silent authentication
Use current Windows user. TraceFinder will not prompt to log in.

Table 1. Security – Global Policy page parameters

Function	Description
Enable Security	Turns on the user security features in the Administrator Console.
Lock Client that Has No Interaction…	Species the number of minutes before an idle TraceFinder session displays a password-protected lock screen and, unless the user enters a user name and password, automatically logs off the user. Range: 1 through 999 minutes Default: 5 minutes
Authenticate Explicit Users Only	Allows login access to only users listed in the Users list on the Users page. See Users.
Silent Authentication	With user security enabled, allows a user who is currently logged in to a local machine to access the TraceFinder application without logging in again.

Users

When security is enabled, use the features on the Security – Users page to create users, assign roles to users, manage role permissions, and map Active Directory groups to TraceFinder roles.

Follow these procedures:

- To open the Users page
- To add a new user
- To remove a user
- To verify a user's group membership

❖ To open the Users page

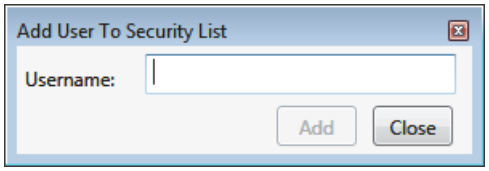
Click **Users** in the navigation pane.

The Security – Users page opens.

❖ To add a new user

1. Click the **Add User** icon, .

   The Add User to Security List dialog box opens.



2. Type the login name of the new user and click **Add**.
3. The application adds the new, unverified, user to the Users list.
   - A green check, , indicates verified users.
   - A red X, , indicates unverified users.
4. To verify that the users in the list are members of the current authentication group, click the **Verify Users** icon, .

5. In the Roles Granted Directly area, select the roles you want to assign to this user.
6. When you have completed all your changes, click **Apply**.

❖ To remove a user

1. Select the user name in the Users list.
2. Click the **Delete User** icon, .

   The application immediately removes the selected user.

❖ To verify a user's group membership

1. Select the user name in the Users list.
2. Click the **Refresh Groups** icon, , in the Roles Via Group Membership area.

   The application displays all groups to which the selected user belongs.

Roles

Use the features on the Security – Roles page to define the roles that are available for users and assign permissions to these roles. This topic describes the default responsibilities for the following default user roles created in the TraceFinder application: Security, LabDirector, ITAdmin, Supervisor, Technician, and QAQC. Each role has default permissions. See "Role Permission Defaults" on page 16. If your team has changed these default permissions, your access might be different. You must also activate user security for these user roles to take effect.

A user in either the default LabDirector or ITAdmin role assigns you to a role that gives you access to specific modes and features of the TraceFinder application. When you log in, the navigation pane displays links to only the modes, interface areas, and features that you have permission to access.

IMPORTANT User roles are in effect only when user security is activated. When user security is not activated, all users have access to all permissions except Security.

These are the default user roles:

- Security
- LabDirector
- ITAdmin
- Supervisor
- QAQC
- Technician

Security

In the Security role, you can access only the Security features on the Administrator Console; you cannot access the TraceFinder application.

LabDirector

In the default LabDirector role, you review graphically applicable data and manipulate data, batches, methods, and instruments.

A laboratory director is responsible for these tasks:

- Creating or editing methods for new levels of detection or adding new compounds to the existing database
- Reviewing data from the mass spectrometer
- Running samples and reviewing data collected by others
- Reporting the data
- Understanding the results and giving final approval of the released data before archiving

ITAdmin

In the default ITAdmin role, you set security, manage users into their roles, and manipulate the various databases. You are responsible for adding compounds into the compound databases.

An IT administrator is responsible for these tasks:

- Handling the databases
- Applying roles to users
- Understanding security, users, and groups
- Creating local users and network groups

Supervisor

In the default Supervisor role, you are responsible for setting up the instrument samples and using previously built sequences and methods for processing and acquiring data. You also develop and edit methods for processing and acquiring data, review the data, and distinguish between the need to rerun samples or pass reports up to the laboratory manager for final review. On a daily basis, you establish the priority for a list of samples to run and create the sequence of events.

A supervisor is responsible for these tasks:

- Submitting samples
- Creating and submitting batches
- Reporting the data to management
- Creating or editing methods for new levels of detection or adding new compounds to the existing database
- Reviewing data from the mass spectrometer
- Understanding the results, who ran the batch, and who passed along the results before giving intermediate approval and sending the data to management
- Modifying new compounds or adjusting methods for specific result sets

QAQC

In the default QAQC role, you review graphically applicable data and interpret the data, but you do not manipulate the data.

A QAQC technician is responsible for these tasks:

- Reviewing data from the mass spectrometer
- Understanding the results and who ran and passed along the results before giving intermediate approval and sending the data to management
- Receiving instructions for new sets of samples for the TraceFinder application to analyze after finishing the current analysis

Note In the QAQC role, you have access only to the Analysis mode.

Technician

In the default Technician role, you are responsible for setting up the instrument samples and using previously built sequences and methods for processing and acquiring data. You also edit existing methods for processing and acquiring data, review collected data, and distinguish between the need to rerun samples or pass reports up to the supervisor. On a daily basis, you are responsible for gathering the list of samples to run and creating the sequence of events.

A technician is responsible for these tasks:

- Submitting samples
- Creating and submitting batches
- Creating data to be reviewed by management
- Receiving instructions for new sets of samples for the TraceFinder application to analyze after finishing the current analysis
- Reviewing data from the mass spectrometer
- Understanding the resulting data, making integration changes, and passing those changes up for further approval

Using the Roles Page

Use the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

Follow these procedures:

- To open the Roles page
- To add a role
- To remove a role
- To change permissions for a role

❖ To open the Roles page

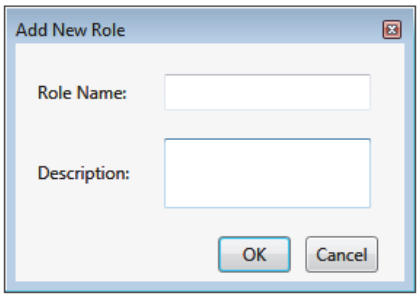
Click **Roles** in the navigation pane.

The Security – Roles page opens. For detailed descriptions of all the parameters on the Roles page, see "Security – Roles" on page 15.

❖ To add a role

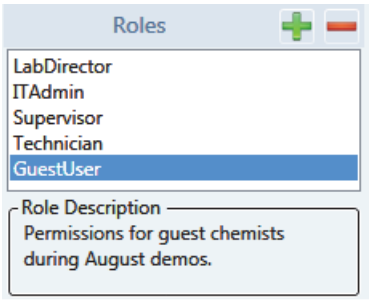
1. Click **Add Role** in the Roles area.

   The Add New Role dialog box opens.



2. In the Role Name box, type a name for the new role.
3. (Optional) In the Description box, type a description for the new user role.

   The application displays the description for a selected role below the Roles list on the Security – Roles page, as in this example:



4. Click **OK**.
5. On the Security – Roles page, select the permissions for the new role.
6. When you have made all your changes, click **Apply**.

Note You cannot open a different page in the Administrator Console while these changes are pending.

❖ To remove a role

IMPORTANT Be careful before deleting the LabDirector or ITAdmin roles. These are the only default roles that can control user security. You must have at least one user role that can control security.

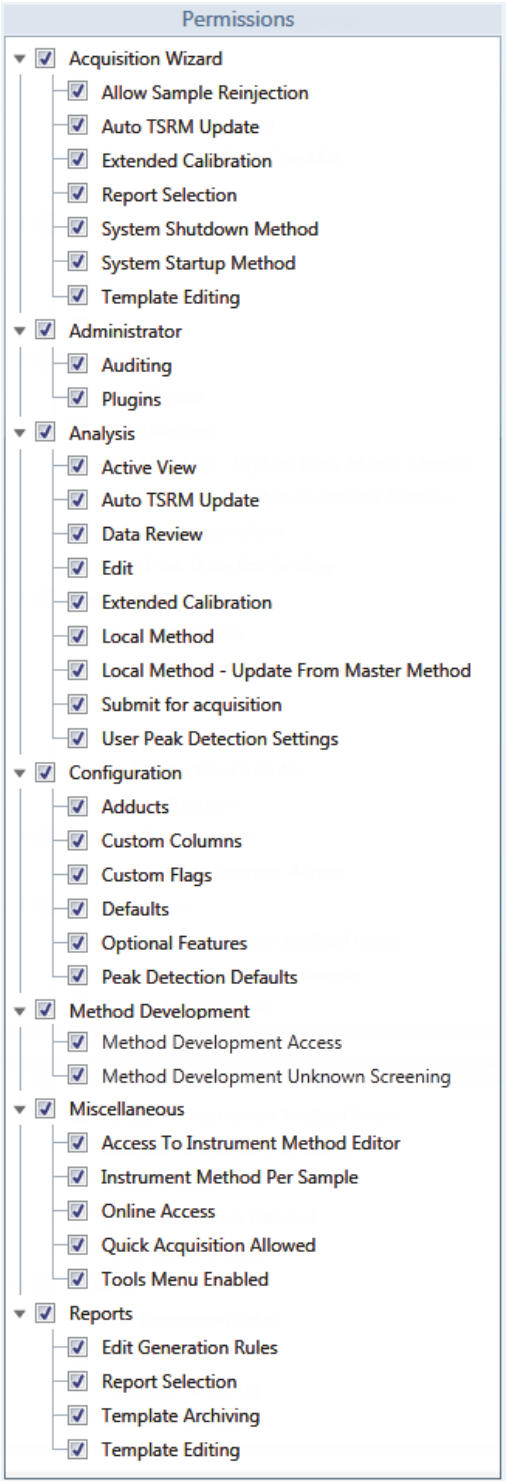
1. Select the role in the Roles list.
2. Click the **Delete Role** icon, .
3. When prompted to confirm this action, click **Yes**.

   The application immediately deletes the specified role. There is no undo for this action.

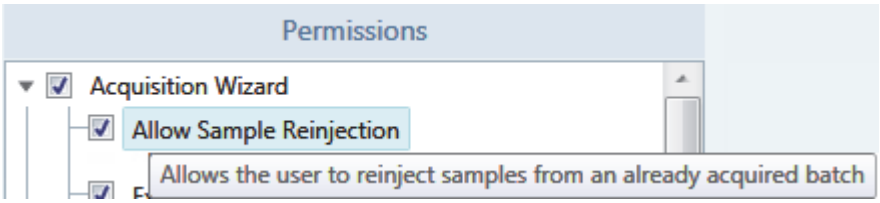
❖ To change permissions for a role

1. Select the role in the Roles list.

   The Permissions list indicates all the permissions assigned to the selected role. The following example shows the default permissions for the LabDirector role:



2. Select the check box for each permission you want to assign to the selected role, or clear the check box for each permission you do not want to assign to the role.
3. To see additional information about a permission, hold your cursor over the permission in the Permissions list.


Permissions
Acquisition Wizard
Allow Sample Reinjection
Allows the user to reinject samples from an already acquired batch

4. To reset all the permissions that were specified before you made changes, click **Undo**.

   The applications discards all pending changes to all the roles.
5. When you have made all your changes, click **Apply**.

   The application saves all pending changes to all the roles.

Security – Roles

Use the features on the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

Figure 2. Security – Roles page

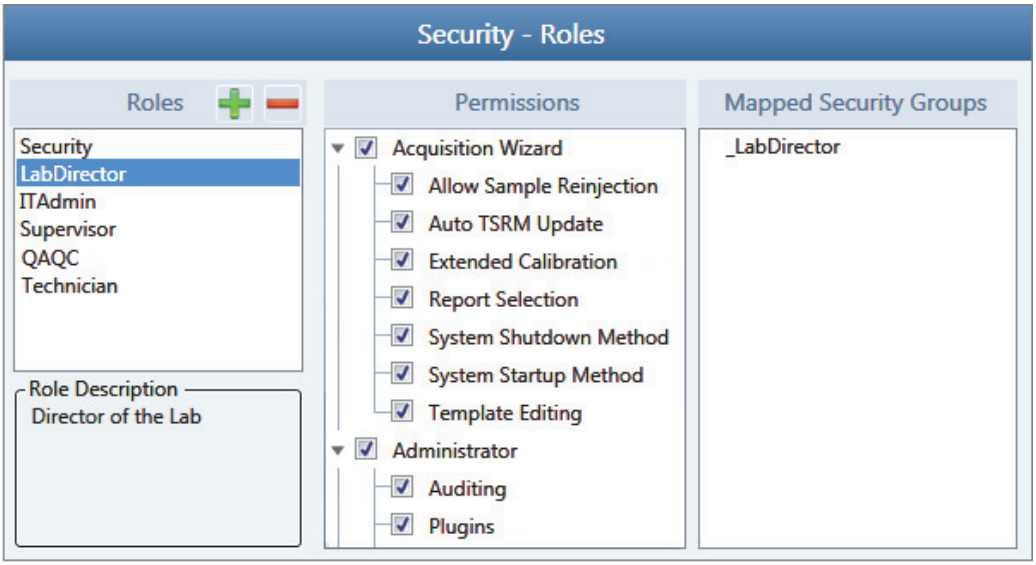


Table 2. Roles page

Function	Description
Roles	Displays all available roles.
Role Description	User-defined description of the selected role.
Permissions	Displays all permissions allowed for the selected role.
Mapped Security Groups	Displays all Windows security groups that are mapped to the selected role. The group inherits all permissions of the roles to which it is mapped. To map a security group to a role, see "Role Mapping" on page 18.

Role Permission Defaults

The following table shows the default permissions assigned to each of the default user roles.

Table 3. Permission defaults (Sheet 1 of 2)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Acquisition Wizard					
Allow Sample Reinjection	✓	✓			
Auto TSRM Update	✓	✓			✓
Extended Calibration	✓	✓			✓
Report Selection	✓	✓			
System Shutdown Method	✓	✓			✓
System Startup Method	✓	✓			✓
Template Editing	✓	✓			
Administrator					
Auditing	✓		✓		
Plugins	✓	✓	✓		
Analysis					
Active View	✓	✓			✓
Auto TSRM Update	✓	✓			✓
Data Review	✓	✓		✓	✓
Edit	✓	✓			✓
Extended Calibration	✓	✓			✓
Local Method	✓	✓			
Local Method – Update from Master Method	✓	✓			
Submit for Acquisition	✓	✓			✓
User Peak Detection Settings	✓	✓			✓
Configuration					
Adducts	✓	✓			
Custom Columns	✓	✓			
Custom Flags	✓	✓			
Defaults	✓	✓			
Optional Features	✓	✓			

Table 3. Permission defaults (Sheet 2 of 2)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Peak Detection Defaults	✓	✓			
Method Development					
Method Development Access	✓	✓			
Method Development Unknown Screening Access	✓	✓			
Miscellaneous					
Access to Instrument Method Editor	✓	✓			
Instrument Method Per Sample	✓	✓			✓
Online Access	✓	✓		✓	✓
Quick Acquisition Allowed	✓	✓			
Tools Menu Enabled	✓	✓		✓	✓
Reports					
Edit Generation Rules	✓	✓			
Report Selection	✓	✓			
Template Archiving	✓	✓			
Template Editing	✓	✓			

IMPORTANT The Security role has access only to the security features on the Administrator Console. Users who are assigned only to this role cannot access other features in the TraceFinder Administrator Console or in the main TraceFinder application.

Role Mapping

Use the features on the Security – Role Mapping page to assign Windows security groups to the default roles or the roles you defined for the TraceFinder application.

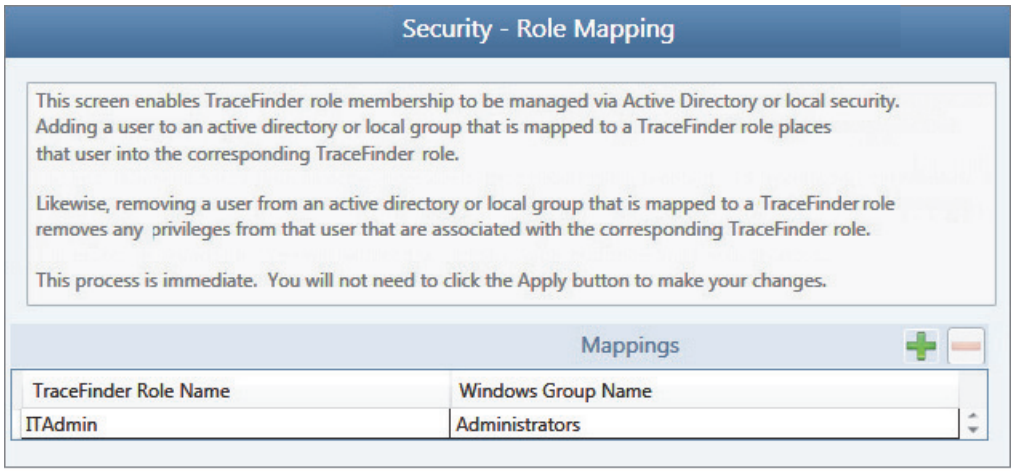
Follow these procedures:

- To open the Role Mapping page
- To create a new mapping

❖ To open the Role Mapping page

Click **Role Mapping** in the navigation pane.

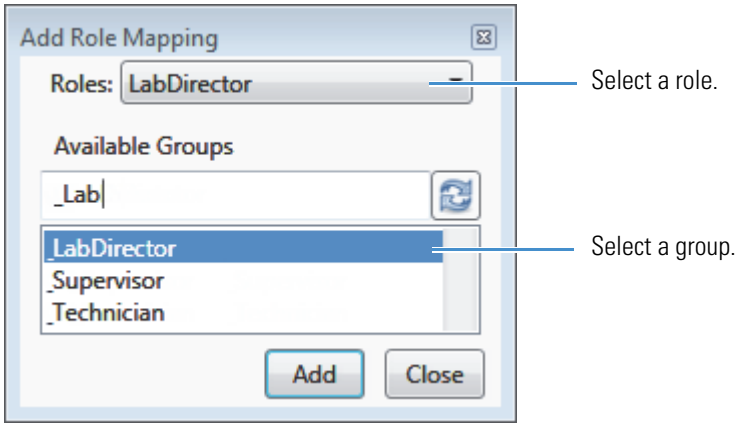
The Security – Role Mapping page opens.


Security - Role Mapping
This screen enables TraceFinder role membership to be managed via Active Directory or local security.
Adding a user to an active directory or local group that is mapped to a TraceFinder role places
that user into the corresponding TraceFinder role.
Likewise, removing a user from an active directory or local group that is mapped to a TraceFinder role
removes any privileges from that user that are associated with the corresponding TraceFinder role.
This process is immediate. You will not need to click the Apply button to make your changes.
Mappings
TraceFinder Role Name
Windows Group Name
ITAdmin
Administrators

❖ To create a new mapping

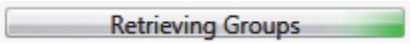
1. Click the **Create Mapping** icon, .

   The Add Role Mapping dialog box opens.



2. If the Available Groups list is not populated, click the **Retrieve Groups** icon, .

   The dialog box displays a progress bar until it finishes searching the Windows Active Directories and displays all the available groups defined for your organization.

   - A user in the default LabDirector role who also has administrator privileges on the local machine can create groups and assign users to those groups.
   - A user in the default LabDirector role who also has administrator privileges on the network can create groups in the Windows Active Directories.

3. Select a role from the Roles list.
4. Select a group from the Available Groups list.

   Tip This list can be very long. To quickly jump to the group you want, begin typing the group name in the text field. The list scrolls to the first matching text string. The search is not case sensitive.

5. Click **Add**.

   The application immediately creates the mapping and closes the Add Role Mapping dialog box.

6. To leave the Role Mapping page, click **Close**.

Using the Repository View

Use the features in the Repository view to specify repositories for batches, methods, and templates that you create.

Contents

- Administration
- Domain Mapping

Administration

Use the features on the Repository – Administration page to create and manage fixed or network drives.

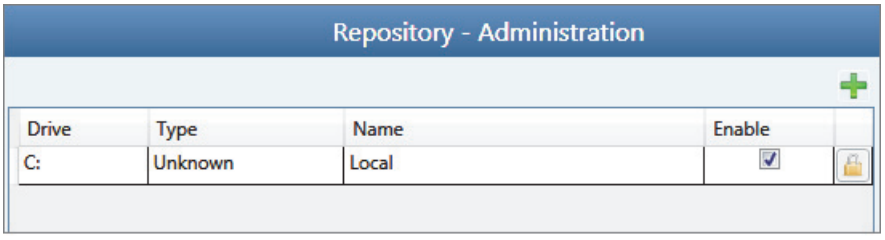
Follow these procedures:

- To open the Repository – Administration page
- To add an available repository
- To create a new repository
- To delete a repository

❖ **To open the Repository – Administration page**

Click **Administration** in the Repository navigation pane.

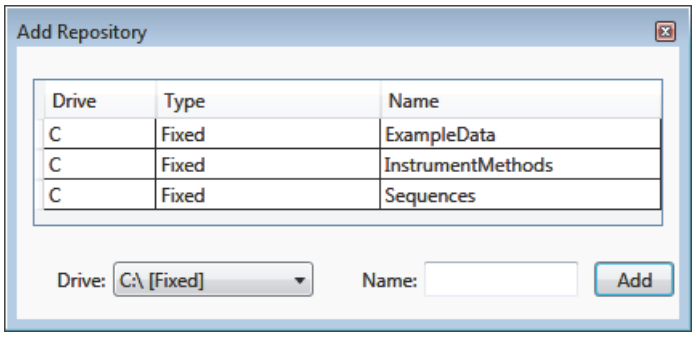
The Repository – Administration page opens.



❖ To add an available repository

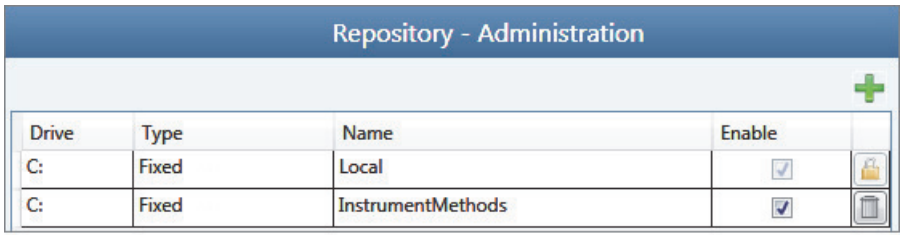
1. Click the **Add Repository** icon, .

   The Add Repository dialog box opens.



2. Select a repository in the list.
3. Click **Add**.

   The Add Repository dialog box closes, and the application adds the selected repository to the available repository list.



4. Make sure the **Enable** check box is selected.

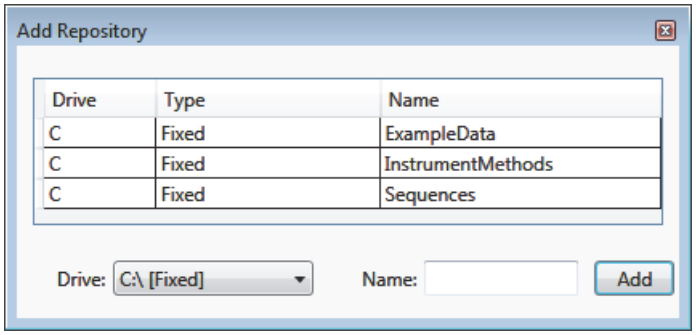
   The application enables all added repositories by default.

5. When you have made all your changes, click **Apply**.

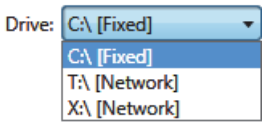
❖ To create a new repository

1. Click the **Add Repository** icon, .

   The Add Repository dialog box opens.



2. Select a drive from the Drive list.



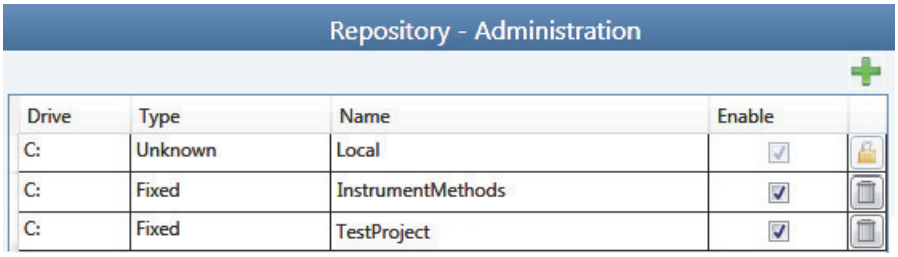
Drives can be any of the following:

- Fixed: Directly connected to your computer.
- Network: Either a remote box or a mapped drive. A shared folder that is mapped to a drive letter might physically exist on your computer, but because it is mapped, it is considered a Network drive.
- Removable: Temporary drives such as a 3.5 in. disk or a USB drive.

Note You cannot save data to a network or removable drive.

3. Type a name for the new repository in the Name box.
4. Click **Add**.

The Add Repository dialog box closes, and the application adds the new repository to the repository list.



5. When you have made all your changes, click **Apply**.

❖ To delete a repository

Click the **Remove Repository** icon, , for the repository you want to delete.

The application immediately removes the repository. There is no confirmation.

Note Using the Undo function does not necessarily return a deleted repository. The Undo function returns the Repository – Administration page to the state when you first opened it or to the state immediately after the last Apply.

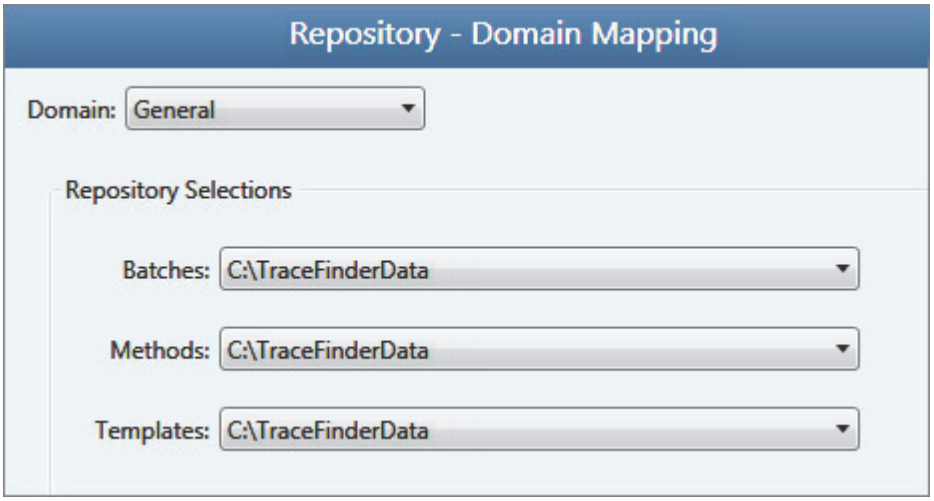
Domain Mapping

Use the domain mapping features to change the drive where you store your data folders, such as batches, methods, and templates (the default location is C:\TraceFinderData). You must use a fixed drive. You cannot save data to a network or removable drive.

❖ To select the drives for storing data folders

1. Click **Domain Mapping** in the Repository navigation pane.

   The Repository – Domain Mapping page opens.



2. Select a domain.
3. In the Repository Selections area, select the repository where you want to save batches, methods, and templates.

   The dropdown lists display the default repository and all available repositories that you added. See "To add an available repository" on page 22 or "To create a new repository" on page 22.

   By default, the application saves batches, methods, and templates to the following folders:

   C:\TraceFinderData\3.3\Projects

   C:\TraceFinderData\3.3\Methods

   C:\TraceFinderData\3.3\Templates

   When you create any of these items in the TraceFinder application, the application creates Projects, Methods, and Templates folders in your specified repositories.

3

Using the Audit View

Use the features in the Audit view to specify the events that are audited, that require confirmation, or that require a sample authorization. You can also specify a list of default reasons for a specific event and whether a user can submit a custom reason.

An event describes a specific action, such as opening or saving a batch, method, or template. Each event can include multiple actions. For example, an "edit" event includes all the changes to the data since the last time the user saved the data.

The TraceFinder application records all user access, including logging in, logging out, data creation and editing (batches, methods, and templates), and manual integration. As a user with Auditing permission, you can configure the auditing service by specifying the events to be logged, the events requiring confirmation, and those that can have custom reasons. In the TraceFinder application, all users can use the Audit Viewer to view the resulting log files to track user access and modifications to the data.

Contents

- Audit Logs
- Event Maps

Audit Logs

The application creates the following audit trail log files:

- Application: All user access, such as starting or stopping the application, logging in, logging out, or accessing data (batches and methods). The application saves the data in the following log file: C:\Thermo\TraceFinder\3.3\Logs\AuditLog.adb.
- Master Method: All user interactions with master methods, such as creating, opening, or editing. The application saves the data in the following log file: C:\TraceFinderData\3.3\Methods*MasterMethodName*\AuditLog.adb.
- Batch Template: All user interactions with batch templates, such as creating, opening, or editing. The application saves the data in the following log file: C:\TraceFinderData\3.3\Templates\Batches*BatchTemplateName*\AuditLog.adb.
- Batch: All user interactions with batches, such as creating, opening, editing, acquiring, processing, or reporting. The application saves the data in the following log file: C:\TraceFinderData\3.3\Projects*SubFolder**BatchName*\AuditLog.adb.

Event Maps

An event map defines which auditing parameters the application uses for each audited event.

Use the following procedures:

- To open the Audit – Administration page
- To create an event map
- To edit an event map

❖ To open the Audit – Administration page

Click **Administration** in the Audit navigation pane.

The Audit – Administration page opens. For a detailed list of all parameters, see "Administration Page" on page 28.

❖ To create an event map

1. Do one of the following:
   - Click the **Create New Map** icon, .

     The application adds a new audit map named *NewMap_1* to the audit map list. The application sets all parameters in the new audit map to the default.

   –or–

   - Select an audit map and click the **Copy** icon, .

     The application copies the selected map and adds a new audit map named *OriginalName*_1 to the audit map list. The application copies all parameter values from the selected map.
2. (Optional) Edit any of the following parameters:
   - Select the audit map name in the Name column, and rename the new audit map.
   - In the Selected Map pane, type information for the new audit map.
   - In the Events pane, edit the parameter values for the new audit map.

❖ To edit an event map

1. In the Audit Maps pane, select the audit map that you want to edit.

   The application displays the parameter values for the selected map in the Events pane.

   Tip The active audit map is not necessarily the selected one. See Distinguishing Active from Selected Maps.

2. Select or clear the check box for each of the following parameters that you want to edit.
   - **Audit**: Available for all event types.
   - **Confirm**: Available for only immediate event types.
   - **Custom Reason**: Available for only immediate event types.
   - **ESignature**: Available for only immediate event types.
3. In the Default Reason columns, enter or change the text.

   This parameter is available for only immediate event types.
4. Click **Apply**.

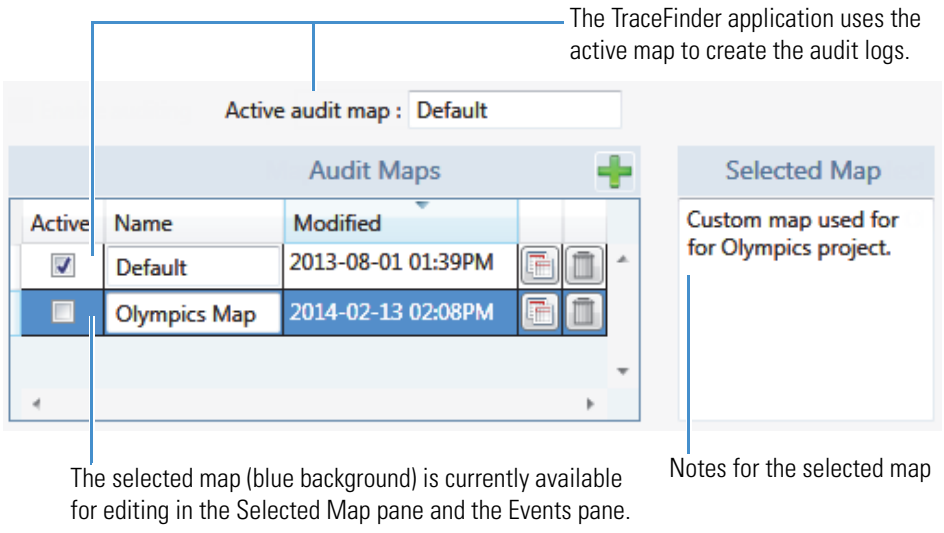
   The application saves your changes to the audit map. When this map is selected as the Active map, the application applies these audit parameter settings to all user interactions. To be sure you know which audit map is the active one, see Distinguishing Active from Selected Maps.

Distinguishing Active from Selected Maps

When you work with event maps, you can edit parameters for the selected map; however, the selected map is not necessarily the active map that the TraceFinder application is using. A selected Active check box indicates an active map; a blue background indicates a selected map.

Use the following graphic to be sure you know the difference.

Figure 3. Difference between active and selected maps


The TraceFinder application uses the active map to create the audit logs.
Active audit map : Default
Audit Maps
Selected Map
Active
Name
Modified
Default
2013-08-01 01:39PM
Olympics Map
2014-02-13 02:08PM
Custom map used for for Olympics project.
The selected map (blue background) is currently available for editing in the Selected Map pane and the Events pane.
Notes for the selected map

Administration Page

Use the features on the Audit – Administration page to specify which events are audited and which auditing parameters you want to use for each audited event.

Figure 4. Administration page

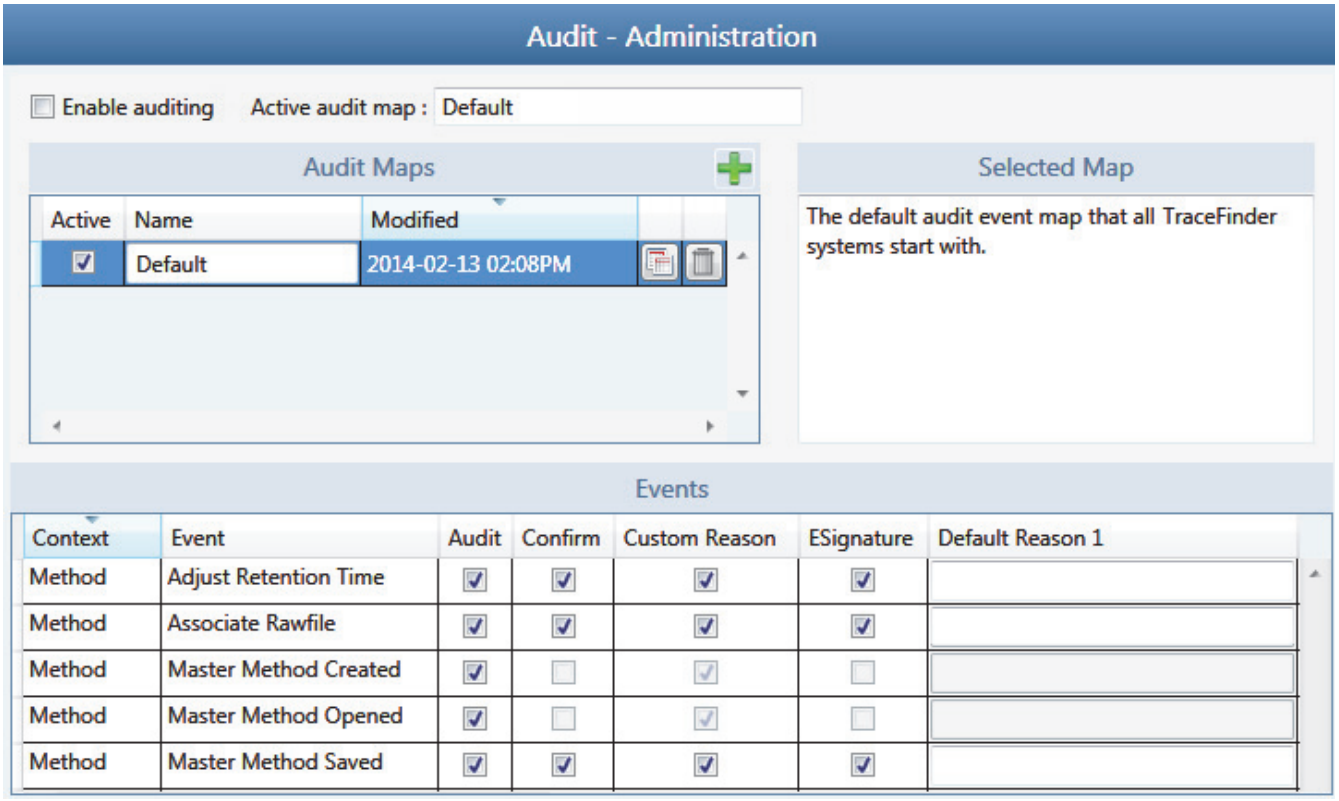


Table 4. Administration page parameters (Sheet 1 of 2)

Parameter	Description
Enable Auditing	Turns on the auditing features in the TraceFinder application.
Active Audit Map	The name of the currently selected audit map.
Audit Maps	
Active	Makes the selected map the currently used map.
Name	Name of the audit map.
Modified	The last date the audit map was edited.
Copy	Copies this audit map to a new name. The default name is *OriginalName*_1.
Delete	Removes the audit map from the list of available audit maps.
Selected Map	Editable description of the currently selected map.

Table 4. Administration page parameters (Sheet 2 of 2)

Parameter	Description
Events	
Context	Events are grouped into application-level, batch-level, template-level, or method-level contexts.
Event	An action that triggers an entry in the audit log. There are three types of events: automatic, immediate, and queued. For a detailed list of events that the application logs, see Events. • For automatic events, the Confirm, Custom Reason, Default Reason, and ESignature features are not available. • For immediate events, all Events features are available. • Queued events—unsaved edits to a batch or method that are recorded in the audit log—require no confirmation, reason, or authorization.
Audit	Writes this event to the audit log.
Confirm	Requires that the user enter a user name, password, and reason before completing this event.
Custom Reason	Allows a custom reason for the event. When prompted to confirm the event, the user can select a reason from the list of default reasons or type a custom reason in the Confirm Changes dialog box.
ESignature	Requires that the user authorize a sample with an electronic signature before completing this event. This authorization and an associated time stamp appear on all reports for this sample.
Default Reason 1-6	Reasons that you define for an event. Users can select one of these default reasons when prompted to confirm the event in the Confirm Changes dialog box.

Table 5. Events (Sheet 1 of 3)

Parameter	Description
Application	All Application events are automatic events. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for these events.
Application Start	Makes an entry in the audit log each time a user launches the TraceFinder application.
Application Stop	Makes an entry in the audit log each time a user closes the TraceFinder application.
Cdb (Database) Updated	Makes an entry in the audit log each time a user updates the compound database.
Security	
Security Changed	Makes an entry in the audit log each time a user modifies the configuration security settings.
User Lockout	Makes an entry in the audit log each time the application locks out the user.
User Login	Makes an entry in the audit log each time a user logs in to the TraceFinder application.
User Login Failed	Makes an entry in the audit log each time a user enters incorrect credentials when logging in to the TraceFinder application.

Table 5. Events (Sheet 2 of 3)

Parameter	Description
Batch	
Adjust Retention Time	Makes an entry in the audit log each time a user modifies the retention time in the local method for any compound in any sample in the batch. To modify the retention times for a single compound in a batch or to modify the retention times for all compounds in a local method. This is an automatic event.
Associate Rawfile	Makes an entry in the audit log each time a user associates a raw data file with a local method for a batch.
Batch Created	Makes an entry in the audit log each time a user creates a new batch. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Batch Exported	Makes an entry in the audit log each time a user exports a batch.
Batch Moved	Makes an entry in the audit log each time a user saves a batch to a new project folder.
Batch Opened	Makes an entry in the audit log each time a user opens a batch. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Batch Saved	Makes an entry in the audit log each time a user saves a batch.
Batch Saved As	Makes an entry in the audit log each time a user saves a batch to a new name. This is not the same as the entry for “Batch Moved” in which a batch is saved to a different project folder, even though it might also be saved to a new name in the new project folder.
Clear Extended Calibration	Makes an entry in the audit log each time a user clears the Extend Calibration feature when submitting a batch.
Extended Calibration	Makes an entry in the audit log each time a user selects the Extend Calibration feature when submitting a batch.
Manual Integration	Makes an entry in the audit log each time a user changes the manual integration settings on the Data Review page in the Analysis mode.
Peak Added Manually	Makes an entry in the audit log each time a user adds a quantitation or confirming ion peak on the Data Review page in the Analysis mode.
Peak Removed Manually	Makes an entry in the audit log each time a user removes a quantitation or confirming ion peak on the Data Review page in the Analysis mode.
Select New Method	Makes an entry in the audit log each time a user selects a local method in the Batch View in the Analysis mode.
Update Local Instrument Method	Makes an entry in the audit log each time a user updates a local instrument method from the master method.

Table 5. Events (Sheet 3 of 3)

Parameter	Description
Update Local Method from Master Method	Makes an entry in the audit log each time a user updates a local method from a master method in the Batch View in the Analysis mode.
Update Master Instrument Method	Makes an entry in the audit log each time a user updates a master instrument method from the local instrument method.
Update Master Method	Makes an entry in the audit log each time a user updates a master method in the Local Method view in the Analysis mode.
Template	
Template Created	Makes an entry in the audit log each time a user creates a new batch template in the Acquisition wizard. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Template Opened	Makes an entry in the audit log each time a user opens a batch template. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Template Saved	Makes an entry in the audit log each time a user saves a batch template.
Method	
Adjust Retention Time	Makes an entry in the audit log each time a user modifies the expected retention time for a single compound or for all compounds in the method.
Associate Rawfile	Makes an entry in the audit log each time a user associates a raw data file with a master method.
Master Method Created	Makes an entry in the audit log each time a user creates a new master method. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Master Method Opened	Makes an entry in the audit log each time a user opens a master method. This is an automatic event. The Confirm, Custom Reason, Default Reason, and ESignature features are not available for this event.
Master Method Saved	Makes an entry in the audit log each time a user saves a master method.
Master Method Saved As	Makes an entry in the audit log each time a user saves a master method to a new name.
Update Global Instrument Method	Makes an entry in the audit log each time a user updates the global instrument method (in the TraceFinderData\3.3\InstrumentMethods folder) from the current master method.
Update Master Method Instrument Method	Makes an entry in the audit log each time a user updates the current master method from the global instrument method (in the TraceFinderData\3.3\InstrumentMethods folder).

Using the Plugins View

Use the features on the Plugins – Administration page to configure available plugins for the TraceFinder application.

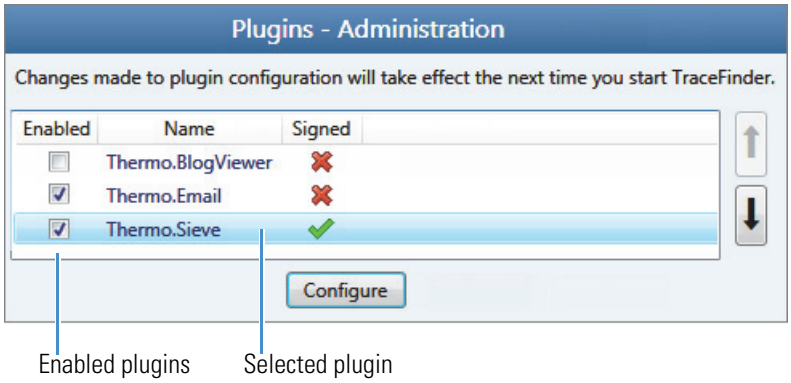
Follow these procedures:

- To enable plugins
- To configure an email plugin
- To configure a Sieve plugin

❖ To enable plugins

1. Click **Administration** in the Plugins navigation pane.

   The Plugins – Administration page opens, listing all available plugins.



2. For each plugin that you want to use in the TraceFinder application, select the **Enabled** check box.

3. To configure a plugin, select the plugin and click **Configure**.

   Note You can configure only one plugin at a time. Do not confuse an *enabled* plugin with a *selected* plugin.

   A dialog box for the selected plugin opens.

   To configure an email plugin, see To configure an email plugin.

   To configure a Sieve plugin, see "To configure a Sieve plugin" on page 35.

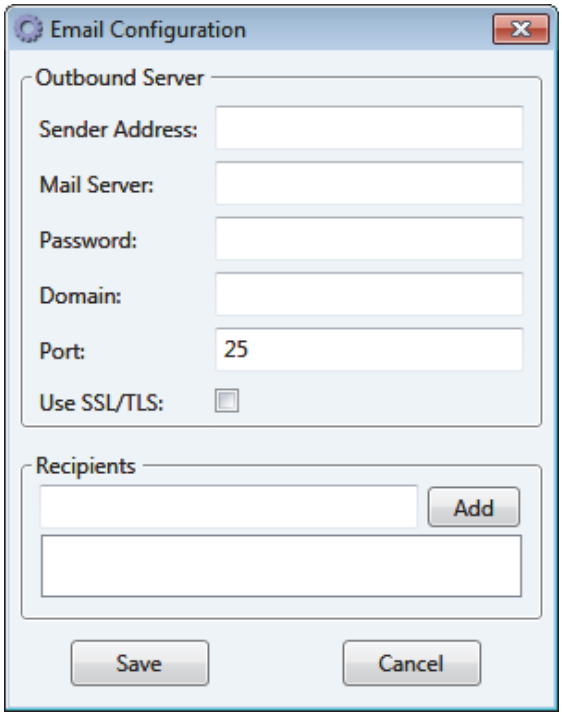
4. In the configuration dialog box, select the options you want to configure and then click **Save**.
5. Click **Apply**.

   The enabled plugins become available the next time you start the TraceFinder application.

❖ To configure an email plugin

1. On the Plugins – Administration page, select the **Thermo.Email** plugin and click **Configure**.

   The Email Configuration dialog box opens.



2. In the Sender Address box, type your complete email address.

   For example: *jane.user@company.com*.

3. Click in the Mail Server box.

   The application automatically fills in the server information.

4. In the Password box, type your user password.

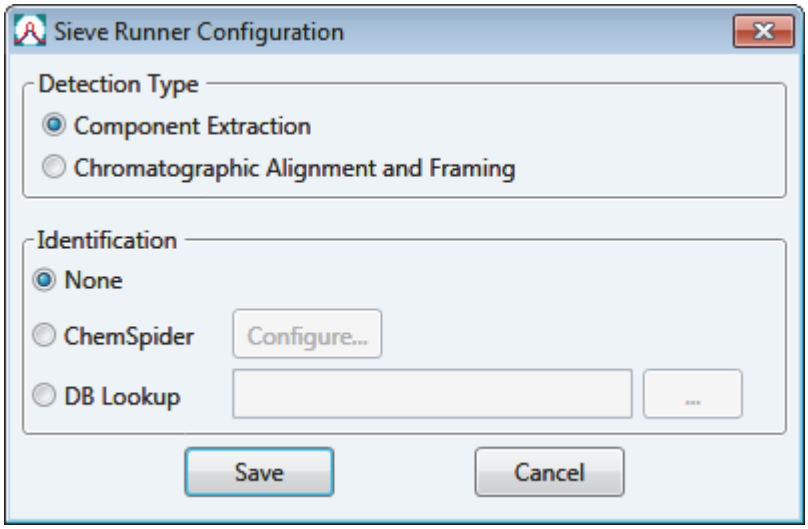
   The application masks your password information.

5. In the Domain box, type your domain.
6. In the Port box, verify that the application automatically filled in the correct port number.
7. To encrypt the communication, select the **SSL/TLS** check box.
8. Click **Save**.

❖ To configure a Sieve plugin

1. On the Plugins – Administration page, select the **Thermo.Sieve** plugin and click **Configure**.

   The Sieve Runner Configuration dialog box opens.



2. In the Detection Type area, select one of the following methods for analyte detection:

   - Component Extraction
   - Chromatographic Alignment and Framing

3. In the Identification area, select one of the following methods for identifying the chemical structure:

   - **None**: Uses no identification method.
   - **ChemSpider**: Uses the ChemSpider web-based chemical structure database search to identify compounds.

     Click **Configure**, select a ChemSpider database, and then specify the mass tolerance, maximum number of frames to identify, and the default ion charge. Then click **Save**.

   - **DB Lookup**: Uses the selected database to identify compounds.

     Browse to locate a Sieve library (.csv), and click **Open**.

4. Click **Save** in the Sieve Runner Configuration dialog box.

Importing and Exporting Administrator Settings

Use the Export button to save your current security settings to a file.

Use the Import button to import saved security settings to your current Administrator Console.

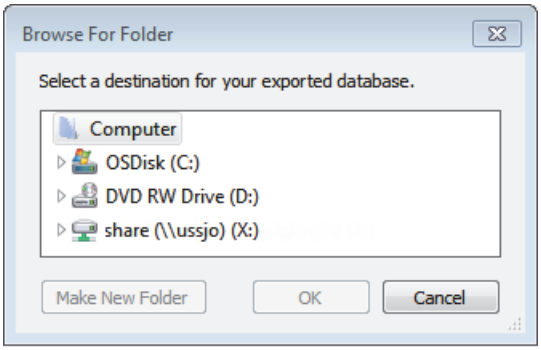
Follow these procedures:

- To export settings to a file
- To import settings from a file

❖ To export settings to a file

1. Set and apply all the settings that you want to export.
2. Click **Export**.

   The Browse For Folder dialog box opens.



3. Locate the folder where you want to save the exported file and click **OK**.

   The target folder can be on the local machine, on a network drive, or on a USB drive.

   Tip To create a new folder for the saved data, navigate to a higher level folder, click **Make New Folder**, type the name for the new folder, and click **OK**.

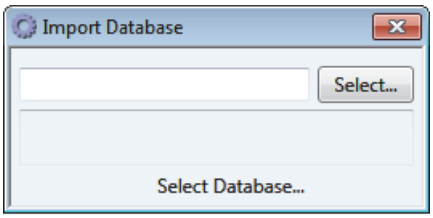
   The application writes the saved security information to the following file:

   AdminConsole.abd

❖ To import settings from a file

1. Click **Import**.

   The Import Database dialog box opens.

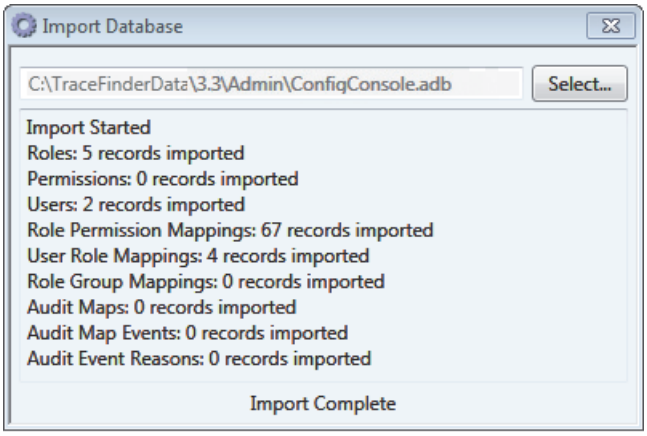


2. Click **Select** and locate a saved administrator database file (.adb) to import.

   The database file can be on the local machine, on a network drive, or on a USB drive.

3. Click **Open**.

   The Import Database dialog box displays the imported records.



4. Close the Import Database dialog box.
5. To see the imported changes on your current page, refresh the page.

Index

A

Active Directory Domain, authentication method 2
AdminConsole.abd 37
authentication, user security 1
automatic screen locking 3

C

contacting us vii

D

default role permissions 16
domain mapping 24

E

exporting administrator settings 37

I

importing administrator settings 38
ITAdmin role 9

L

LabDirector role 8
Local Windows, authentication method 1
logging in when user security is enabled x
logging in when user security is not enabled viii

M

mapping, roles 18

P

parameters
- Authenticate Explicit Users Only 5
- Enable Security 5
- Lock Client that Has No Interaction 5
- Silent Authentication 5

Plugins – Administration page 33
procedures
- add a new user 6
- add a role 11
- add an available repository 22
- allow a single-access login 4
- change permissions for a role 13
- configure a Sieve plugin 35
- configure an email plugin 34
- create a new mapping 18
- create a new repository 22
- create an event map 26
- delete a repository 23
- edit an event map 26
- enable automatic screen locking 3
- enable plugins 33
- enable security 3
- export settings to a file 37
- import settings from a file 38
- open the Audit – Administration page 26
- open the Global Policy page 3
- open the Repository - Administration page 21
- open the Role Mapping page 18
- open the Roles page 11
- open the Users page 6
- open TraceFinder Administrator Console Help vi
- remove a role 12
- remove a user 7
- restrict access only to users created in TraceFinder 4
- select the drives for storing data folders 24
- specify how user authentication is implemented 1
- verify a user's group membership 7
- view TraceFinder documents using the Start menu vi

Q

QAQC role 10

R

Repository – Administration page 21
Repository – Domain Mapping page 24

role mapping 18
role permission defaults 16
role permissions, default 16
roles
  ITAdmin 9
  LabDirector 8
  QAQC 10
  Security 8
  Supervisor 9
  Technician 10

S

screen locking, automatic 3
Security – Authentication Provider page 1
Security – Global Policy page 5
Security – Role Mapping page 18
Security – Roles page 11
Security – Users page 6
Security role 8
Supervisor role 9

T

Technician role 10

U

user security, enabling 3